简译版

减轻老旧应用的威胁

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	How to diminish the great threat of legacy apps		
原文作者	Tim Buntel	原文发布日期	2019 年 5 月 28 日
作者简介	Tim Buntel 是 Threat Stack 应用安全副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/05/28/legacy-apps-threat/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

减轻老旧应用的威胁

Tim Buntel

2019 年 5 月 28 日

美国征信巨头 Equifax 的数据泄漏事件突显了未修复漏洞的软件应用所带来的严重风险。在此次事件中，攻击者利用了 Apache Struts 的一个已知漏洞，成功窃取了 1.46 亿条客户记录。如今的现实情况是，企业使用越来越多的商业和自开发应用；而在为这些应用维护适当的安全补丁方面，企业面临着诸多挑战。

当考虑到不再受监控或维护的老旧应用时，企业面临的挑战就更加严峻了。攻击者很乐意使用任何必要的手段来访问企业的网络，如果企业没有全面的安全计划来解决老旧应用问题，则这些应用会成为他们理想的攻击向量。

大多数企业和组织的技术堆栈中都有被遗忘的老旧应用——这是企业生命周期中相当典型的一部分。随着企业的成长，他们会遇到越来越多的挑战，承受着跟上发展和业务目标的沉重负担。随着工作流程和优先级的转变，不必要的应用可能会被遗忘，但却未从技术堆栈中删除。对企业来说，像这样的安全盲点会带来巨大的风险。

减轻老旧应用的风险并非易事，企业需要做大量的工作并提前进行规划。以下是确保良好应用安全状态的一些最佳实践。

利用现有的标准和法规

进行全面的安全审计费时费力。为了减轻负担，企业可以利用所有的可用资源。例如，企业可以根据当前的合规性法规（如 GDPR）对老旧代码进行审计——已建立的安全要求可帮助企业实现可靠的安全性。当然，企业应该根据自身情况对这些通用法规进行裁剪，以适合自身业务需要。

维护准确的应用清单

企业无法修复看不到的东西。因此，他们应创建并维护准确的应用清单，并定期更新该清单。该清单应列出所有的应用及其依赖项，包括第三方应用。此外，企业应了解这些应用的主要用途并为它们分配管理员。管理员应该了解这些应用的使用情况，并在企业不再需要

它们时及时从技术堆栈中将其删除。

定期解决技术问题

企业的开发团队应分配时间进行持续的技术维护。不断更新、监控和维护现有应用和老旧应用可能会非常麻烦，因此企业应将其作为一项工作，指派部分开发人员定期解决此类问题，以免问题积压。

制定老旧应用的处理策略

当企业进行安全审计和解决技术问题时，很可能会发现不再需要的老旧应用。随着企业的发展和新工作流程的开发，当老旧应用的用例不复存在时，必须将其删除——企业应创建内部流程来实现这一点。确保应用的管理员知道它们要被删除，并能进行配合。此外，一旦将应用从企业的技术堆栈中移除，还要记得从应用清单中将其删除。

全面的安全方法必须涵盖技术基础设施的各个方面。开发团队很容易遗忘老旧应用，但攻击者却不会。老旧应用的漏洞会为寻求任何机会访问企业网络的攻击者提供简单的入口点。

开发团队的时间有限，而网络安全技能差距的扩大也在加剧这一问题。此类挑战越来越严峻，企业必须想办法予以解决。

如果企业未建立和遵守相关的准则和规程 ,则不必要的老旧应用很容易遗留在技术堆栈中，使企业面临严重的风险。采用上述最佳实践，企业可以降低老旧应用的风险，确保其技术堆栈中的某些废弃应用不会沦为攻击入口。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*